REMARKS

Claims 1-13 are currently pending. An amendment to claim 10 has been made to add a subscript immediately before the period ending the claim. Applicant respectfully requests entry of this amendment as it does not raise new issues or further search and places the claims in better form for appeal. It is respectfully submitted that no new matter has been added.

Applicant's response to the Patent Office's remarks in paragraphs 9-15 (pages 2-4 of the Final Office Action mailed January 24, 2006) follows the discussion of the rejection of the claims by the prior art of record.

It appears that the Patent Office has reiterated verbatim the prior Office Action's prior art rejections. The only arguments to Applicant's arguments in the response dated November 4, 2005, presented by the Patent Office, appears to be in paragraphs 9-15, of which paragraphs 9-11 appear to be general statements that Applicant addresses below. Applicant also addresses remaining paragraphs 12-15 below and further differentiates the claimed invention from the prior art of record.

Applicant believes that the finality of the last Office Action is premature. Applicant further requests guidance from the Patent Office regarding the filing of a request for a **Pre-Appeal Brief Conference**. According to the Applicant's understanding, this is a pilot program initiated in July 2005 that has recently been extended.

The present invention concerns plaintext, ciphertext test pairs and is directed to a method for detecting compromise of cryptographic operations because the ciphertext generated by a first cryptographic algorithm from a test plaintext indicates that an apoptosis key has been used (page 4, lines 3-5 and 24-27). Upon detection of an apoptosis key by the generation of ciphertext corresponding to that apoptosis key encrypting the designated plaintext, cryptographic algorithms should be switched (page 4, lines 27-35). An advantage of the solution of the present invention is "that there is no need for controlling respectively trusting the manufacturer or a security service" (page 5, lines 11-12).

The Patent Office rejected claims 1, 3, 5, 7, 8, 10, 11, and 13 under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (US Patent Number 6,327,661) and further in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services).

The Patent Office asserted (page 4-5 of the Final Office Action mailed January 24, 2006) "Regarding claim 1, Kocher teaches a cryptographic system comprising first cryptographic algorithm means for enabling cryptographic operations (column 2, lines 60-67, column 13, lines

20-67), input/output means for receiving input streams and sending output streams (column 13, lines 20-67, column 14, lines 61-67), wherein said input streams are transformed to said output streams by said cryptographic operations (column 13, lines 20-67), at least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i (column 13, lines 20-67), receiving means for receiving a control stream (column 13, lines 20-67, column 14, lines 1-60), checking means for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (column 13, lines 20-67), switching means for stopping said cryptographic operations with said first cryptographic algorithm means (column 13, lines 20-67), wherein said stopping by said switching means is triggered by said checking means (column 13, lines 20-67). Kocher does not expressly disclose including at least one apoptosis key K_i. Kocher teaches self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Kocher (column 2, lines 60-67) discloses "...The following sections describe various embodiments of a general technique of using unpredictable information to protect cryptographic systems (cryptosystems) against external monitoring attacks..."

Kocher (column 13, lines 20-67) discloses "Cryptographic operations should normally be checked to ensure that incorrect computations do not compromise keys or enable other attacks. Cryptographic implementations of the present invention can be, and in a preferred embodiment are, combined with error-detection and/or error-correction logic to ensure that cryptographic operations are performed correctly. For example, a simple and effective technique is to perform cryptographic operations twice, ideally using two independent hardware processors and/or software implementations, with a comparison operation performed at the end to verify that both produce identical results. If the results produced by the two units do not match, the failed comparison will prevent the defective processing result from being used. In situations where security is more important than reliability, if the compare operation ever fails (or fails too many

times) the device may self-destruct (such as by deleting internal keys) or disable itself. For example, a device might erase its key storage memory if either two defective DES operations occur sequentially or five defective DES results occur during the lifetime of the device. In some cryptosystems, full redundancy is not necessary. For example, with RSA, methods are known in the background art for self-checking functions that can be incorporated into the cryptosystem implementation (e.g., RSA signatures can be verified after digital signing operations). Detection of conditions likely to cause incorrect results may also be used. In particular, active or passive sensors to detect unusually high or low voltages, high-frequency noise on voltage or signal inputs, exposure to electromagnetic fields and radiation, and physical tampering may be employed. Inappropriate operating conditions can (for example) trigger the device to reset, delete secrets, or self-destruct. Self-diagnostic functions such as a POST (power-on-self-test) should also be incorporated to verify that cryptographic functions have not been damaged. In cases where an ATR (answer-to-reset) must be provided before a comprehensive self-test can be completed, the self-test can be deferred until after completion of the first transaction or until a sufficient idle period is encountered. For example, a flag indicating successful POST completion can be cleared upon initialization. While the card is waiting for a command from the host system, it can attempt the POST. Any I/O received during the POST will cause an interrupt, which will cancel the POST (leaving the POST-completed flag at zero). If any cryptographic function is called, the device will check the POST flag and (if it is not set) perform the POST before doing any cryptographic operations."

Kocher (column 14, lines 61-67) discloses "A cryptographic processing device for securely performing a cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret by external monitoring, comprising: (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) a source of unpredictable information; (c) a processor: (i) connected to said input interface for receiving and cryptographically processing said quantity, (ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by modifying said sequence; and (d) an output interface for outputting said

cryptographically processed quantity to a recipient thereof."

Kocher discloses (column 14, lines 1-60) "The present invention is extremely useful for improving security, particularly in environments and applications with difficult engineering requirements, by enabling the construction of devices that are significantly more resistant to attack than devices of similar cost and complexity that do not use the present invention. Also, multiple security techniques may be required to make a system secure. For example, leak minimization and obfuscation may be used in conjunction with other security methods or countermeasures. As those skilled in the art will appreciate, the techniques described above are not limited to particular host environments or form factors..."

Kocher does not disclose or fairly suggest "ciphertext," "test plaintext," "test ciphertext," "an apoptosis key," "a control stream," "checking means," "receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i," "switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6)," nor "checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i".

The Patent Office, with reference to independent claims 5 and 11, asserted that column 2, lines 60-67 and column 3, lines 1-10, provide a teaching for the limitation of "implementing within said cryptographic system a first cryptographic algorithm enabling said cryptographic operations" (claim 5) and "which instructions, when read by a computer, enable the computer to perform a first cryptographic algorithm that is enabling said cryptographic operations" (claim 11).

Kocher discloses (column 2, line 60, through column 3, line 10) "The following sections describe various embodiments of a general technique of using unpredictable information to protect cryptographic systems (cryptosystems) against external monitoring attacks..."

The cited passage of Kocher (column 2, line 60, through column 3, line 10) does not

appear to disclose a first cryptographic algorithm.

The Patent Office asserted that Kocher discloses "checking means for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (column 13, lines 20-67)."

Specifically, claim 1 recites "checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i, switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6)."

Claim 5 recites "selecting at least one test plaintext P_i and enciphering each test plaintext P_i with said first cryptographic algorithm and with a corresponding apoptosis key K_i thereby generating a corresponding test ciphertext C_i for each test plaintext P_i , implementing within said cryptographic system (1) said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i, implementing within said cryptographic system (1) receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i , implementing within said cryptographic system (1) checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i, implementing within said cryptographic system (1) switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm, wherein said stopping by said switching means (7) is triggered by said checking means (6).

Claim 8 recites "checking whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i, stopping said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said

first cryptographic algorithm when using said apoptosis key K_i."

Claim 11 recites "check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i, stop said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i.

In the claimed invention, if the test ciphertext corresponds to the test plaintext that results from the apoptosis key, the first cryptographic algorithm is stopped.

Kocher does not disclose checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i. Furthermore, Kocher does not disclose test plaintext, test ciphertext pairs. Instead, Kocher (col. 13, lines 20-67) discloses cryptographic operations should normally be checked to ensure that incorrect computations do not compromise keys or enable other attacks. Kocher discloses a technique of performing cryptographic operations twice, ideally using two independent processors and/or software implementations, with a comparison operation performed at the end to verify that both produce identical results. Kocher discloses, in situations where security is more important than reliability, the device may disable itself or self-destruct (e.g., by deleting internal keys) if the comparison of two cryptographic operations fails. In contrast, applicant discloses the stopping of a first cryptographic algorithm if a test ciphertext is generated for a test plaintext that corresponds to an apoptosis key. Kocher does not disclose or suggest the checking using a test plaintext, a test ciphertext, and an apoptosis key, as has been claimed.

Tschudin discloses a need for a self-destruction mechanism inside a distributed mobile service (abstract). Tschudin discloses the execution of a self-destruction routine that depends on "environmental data" as requested by a read() instruction and provides an example of apoptosis in response to the decryption, via a key, of code encrypted at an originator's site (section 3.1) and then processed at the executing site. Tschudin does not disclose or suggest the checking using a

test plaintext, a test ciphertext, and an apoptosis key, as has been claimed.

Although Kocher and Tschudin are both concerned with cryptographic techniques, their disclosed approaches are starkly different. Kocher checks internally for security compromises in a smartcard environment (e.g., checking for discrepancies between two test results) while Tschudin is vigilant for a kill message to arrive from an external source in a distributed mobile service environment. Kocher discloses multiple cryptographic operations using encryptors that yield results that are later compared whereas Tschudin checks for and decrypts an encrypted kill message that leads to termination of distributed services. Kocher also does not disclose a decryptor that has been relied upon by Tschudin to check for an apoptosis message. Accordingly, Kocher does not readily lend itself to modification by Tschudin.

Furthermore, neither Kocher nor Tschudin disclose or fairly suggest "ciphertext," "test plaintext," "test ciphertext," "an apoptosis key," "a control stream," "checking means," "receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i," "switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6)," nor "checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i".

The Patent Office asserted (page 5, lines 3-9 of the Final Office Action mailed January 24, 2006) "Kocher et al. do not expressly disclose including at least one apoptosis key K_i. Kocher et al. teach self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5)."

Neither Kocher nor Tschudin disclose or suggest an apoptosis key, as claimed, or the claimed technique which determines the existence of an apoptosis key, considered a compromise

situation, when a test plaintext generates a corresponding test ciphertext under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i . Thus, claims 1-13 are not made obvious by Kocher and Tschudin, either alone or in combination.

The Patent Office asserted (page 6, last two lines, through page 7, line 6, of the Final Office Action mailed January 24, 2006) "Regarding claim 7, the combination of Kocher et al. and Tschudin does not expressly disclose publishing said at least one test plaintext P_i and for each test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i. However, Examiner takes Official Notice that publishing information was conventional and well known at the time the invention was made. Furthermore, Kocher et al. stores plaintext and ciphertext prior to comparing them. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to publish this information since Examiner takes Official Notice that it was conventional and well known."

Applicant had challenged the Patent Office on the taking of Official Notice and had requested a teaching applicable to Kocher and Tschudin (or other asserted reference or combination of references) that allegedly discloses or makes obvious claim 7 including limitations from base claim 5 and specifically requests a teaching for the limitation of "the step of publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i."

The Patent Office asserted (page 4, lines 3-6, of the Final Office Action mailed January 24, 2006) "In response to Applicant's request for a reference that teaches publishing information, Examiner submits US Patent 4,634,807, to Chorley et al. (hereinafter Chorley). Chorley teaches publishing a plaintext message and its corresponding encrypted text (column 3, lines 1-67)."

Chorley discloses (column 3, lines 1-67) "software are operating system independent. The protected module simply forms part of a software package and may be in a language common to all such packages. The unencrypted part of the software is tailored to run on a particular operating system, this part being changed as required for different operating systems. A description of the DES is given in Federal Information Processing Standard, No. 46, US

National Bureau of Standards, 15th Jan. 1977. As mentioned previously, the DES key used to encrypt a message must also be used in decrypting it. **On the other hand, a public-key system is one in which encryption can be carried out using one key, but decryption is carried out using a different key. Knowledge of the encryption key, a plaintext message and its corresponding encrypted text does not, in practice, determine the key used to decrypt the ciphertext, and therefore publishing the encryption key does not significantly decrease the security of its corresponding secret decryption key. ...**"

Applicant does not understand how this particular passage discloses or fairly suggests the claim limitation of "the step of publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i." The most relevant part of the cited passage of Chorley reads "On the other hand, a public-key system is one in which encryption can be carried out using one key, but decryption is carried out using a different key. Knowledge of the encryption key, a plaintext message and its corresponding encrypted text does not, in practice, determine the key used to decrypt the ciphertext, and therefore publishing the encryption key does not significantly decrease the security of its corresponding secret decryption key." There appears to be no disclosure of "publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i." **Applicant requests that the Patent Office particularly point out how this passage from Chorley, other passages from Chorley, or other prior art meets this claim limitation.** Absent such a showing, Applicant believes that claim 7 would be allowable for this additional reason.

The Patent Office rejected claims 2, 4, 6, 9, and 12 under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. and Tschudin as applied to claims 1, 5, 8, and 11 above and further in view of Esserman et al. (US Patent Number 5,144,664).

Kocher discloses redundancy to determine security compromises through encryption and relates to a smartcard environment. Tschudin discloses checking for a kill signal through decryption and relates to distributed mobile services. Esserman discloses switching encryptors having different security algorithms and relates to broadcasting TV signals. Even if Kocher were combinable with Esserman, one of ordinary skill would not look to Tschudin as Kocher is

concerned with encryption and the methodology of Tschudin entails decryption.

Furthermore, none of the references Kocher, Tschudin, or Esserman disclose or suggest an apoptosis key, as claimed, or the claimed technique which determines the existence of an apoptosis key, considered a compromise situation, when a test plaintext generates a corresponding test ciphertext under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i . Thus, claims 2, 4, 6, 9, and 12 are not made obvious by Kocher, Tschudin, or Esserman, alone or in combination.

Regarding the remarks in paragraphs 9-15 of the Final Office Action mailed January 24, 2006. As to paragraphs 9 and 10, Applicant has pointed out patentable distinctions between the claimed invention and the prior art of record. As to paragraph 11, Applicant has pointed out mutual differences between Kocher and Tschudin as well as question the modification of Kocher by Tschudin. **As to paragraph 12, Applicant strongly disagrees. There has been no admission. In fact, Applicant has pointed out further differences between the cited prior art and the claimed invention and is willing not to challenge the Patent Office's indication of a deficiency in Kocher** (e.g., page 5, lines 3-4, of the Final Office Action mailed January 24, 2006). Tschudin, in section 3.1, does not disclose or fairly suggest "ciphertext," "test plaintext," "test ciphertext," "an apoptosis key," "a control stream," "checking means," "receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i," "switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6)," nor "checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i".

As to paragraph 13, Applicant discloses (page 4, lines 27-29, of the Specification as filed) "If at some later date, at least one apoptosis key K_i is presented to the cryptographic system which has the property that C_i is the enciphered image of P_i under K_i, then the algorithm could be broken and should not be used anymore." Applicant does not believe that the prior art of record teaches or makes obvious Applicant's invention as currently claimed.

The purpose of paragraph 14 is not understood. Applicant requests that any prior art the

Patent Office deems to meet the limitations of the Applicant's claimed invention be presented.

As to paragraph 15, Applicant discusses, in the above paragraphs, the deficiency of Chorley as a teaching for the limitation of "the step of publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i."

The Examiner is respectfully requested to reconsider and remove the rejections of the claims under 35 U.S.C. 103(a) of 1, 3, 5, 7, 8, 10, 11, and 13 based on Kocher, U.S. Patent No. 6,327,661, in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services) and the claims 2, 4, 6, 9, and 12 based on Kocher, U.S. Patent No. 6,327,661, in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services) and further in view of Esserman, US Patent Number 5,144,664, and to allow all of the pending claims 1-13 as now presented for examination. An early notification of the allowability of claims 1-13 is earnestly solicited.

S.N.: 10/058,661
Art Unit: 2136

Respectfully submitted:

Walter J. Malinowski April 3, 2006

Walter J. Malinowski Date

Reg. No.: 43,423

Customer No.: 29683

HARRINGTON & SMITH, LLP
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203)925-9400, extension 19
Facsimile: (203)944-0245
email: wmalinowski@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

4-3-06 Ann Okrentowich

Date Name of Person Making Deposit